



DEPUTY **SECRETARY** OF DEFENSE

1010 **DEFENSE** PENTAGON  
WASHINGTON, DC 20301-1010



DEC 2 11999

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING  
ASSISTANT SECRETARIES OF DEFENSE  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DEFENSE FIELD ACTIVITIES

SUBJECT: Office of the Secretary of Defense (OSD) Network Security Policy

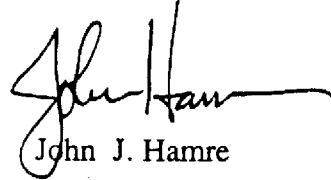
The Department of Defense Chief Information Officer (DoD CIO) recently consolidated the OSD Information Technology (IT) infrastructure into a single information Enterprise. This new Enterprise will include a common architecture, interoperable open standards, standardized common applications and processes, and improved security. As the DoD CIO continues to assess system vulnerabilities, the security architecture will be revised accordingly. This memorandum addresses areas where security vulnerabilities have been identified.

In the past, system vulnerabilities were introduced into the OSD enclaves for the sake of expediency and convenience based upon an acceptable level of risk. These vulnerabilities were associated with Internet web technologies and remote access solutions used to provide information and services to remote OSD users, outside organizations, and the public.

From this point-forward, security should be a primary OSD concern for all IT systems, whether deemed as general purpose or mission critical. Any system could contain sensitive information that needs to be safeguarded. Therefore, implementation of the Defense-In-Depth security approach is required for all IT systems supported by OSD. This security approach utilizes multiple layers of physical and logical protection combined with intrusion detection systems that monitor each layer. Implementing the Defense-In-Depth posture will mitigate the risks to OSD assets.

01 8139 /99

Effective immediately, all modifications to OSD IT systems must conform to the Defense-In-Depth approach. This includes networks, domain name services, public servers, and external access capabilities. The attached appendix contains the implementation guidance. Any exceptions to the stated policy provisions must be approved by the DoD CIO in writing.

A handwritten signature in black ink, appearing to read "John Hamre", with a long horizontal flourish extending to the right.

John J. Hamre

Attachment

# OFFICE OF THE SECRETARY OF DEFENSE (OSD) NETWORK SECURITY POLICY

1. Introduction. This document specifies the policy for securing the OSD network Enterprise. OSD is complying with the Global Information Grid (GIG) Information Assurance (IA) standards by adopting a Defense-in-Depth strategy to provide information assurance across the information Enterprise. The Defense-in-Depth strategy requires varying levels and types of security to be implemented to protect information and services (e.g., firewalls, Public Key Infrastructure [PKI], virtual private networks [VPNs], encryption, access control, etc.), to detect attacks (e.g., intrusion detection systems [IDS]), and to quickly respond (e.g., counter measures). The Department of Defense (DoD) Chief Information Officer (CIO) has developed this policy document to address areas where security vulnerabilities have been identified.

2. Purpose. The purpose of this document is to provide guidance to protect the confidentiality and security of all OSD data, systems, and networks and to mitigate the risk of unauthorized access.

3. Policy.

3.1 DoD CIO-approved firewalls will be established and maintained at each enclave and at the OSD Enterprise connection. OSD proxy and application gateways will be established for each enclave.

3.2 The use of non-OSD domains will be terminated in the OSD enclave networks. All OSD enclaves will **use an** *"\*.osd\*.mil"* domain naming convention, be sponsored by an OSD component, and will be approved by the **DoD** CIO.

3.3 All support for non-OSD organizations from inside the OSD enclave will be terminated. All resources and services accessed by non-OSD enclave users will be hosted in the OSD De-Militarized Zone (DMZ). Non-OSD organizations will not be provided with OSD Domain Name System (DNS) services.

3.4 The hosting of public servers from within the OSD enclave will be terminated. All public servers will be hosted outside of the OSD network, for example, OSD DMZ and Defense **Technical Information Center (DTIC)**.

3.5 All internal dial up connections to the resources, services, and systems in the OSD enclave will be terminated and moved to the OSD DMZ. Dial up connections will be secured using a method approved by the **DoD** CIO.

3.6 All unsecured connections between remote OSD locations (e.g., the Pentagon and Crystal City) will be secured in a manner approved by the **DoD** CIO. All connections to assets outside the OSD enclave will pass through secured interface points.

3.7 Intrusion detection systems will be implemented to monitor each layer of the physical and logical protection.

3.8 Configuration management of OSD information systems and networks will be implemented.

3.9 All security devices, products, firewalls, and firewall policies used by OSD will be in accordance with (IAW) the GIG IA standards and approved by the DoD CIO.

3.10 Measures will be taken to secure all information systems to the maximum extent possible and to block malicious mobile code in an effort to mitigate adverse impact to OSD systems. Security measures will be IAW the GIG IA standards and approved by the DoD CIO.

#### 4. Security Incident Reporting.

4.1 Security incident reporting will be IAW the GIG IA standards and the DoD CIO standard procedures.

-